would permit copying, alteration or sharing of the decrypted file. Even if someone were to succeed in altering the information contained within the original plaintext file, any forgery or fraud could be easily detected by comparing the altered copy with the originally stored file.

The special software may be supplied by courier in the form of a tangible recorded copy (*e.g.*, a CD-ROM or floppy disk) or by means of a secure, password-protected network communication between server and client computers.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

1. A method for protecting an electronic file from unauthorized access, copying or alteration, comprising:

(a) providing a plaintext file that includes blocks of original binary data to be encrypted, said blocks having a given length and a maximum possible integer value;

(b) providing a first key that includes a number of indexed integer values selected from a set bounded below by 0 or 1 and above by the maximum possible integer value of the blocks of binary data to be encrypted;

(c) providing a second key that includes a number of indexed integer values selected from a set bounded below by 0 and above by the predetermined number of indexed integer values included in the first key;

(d) providing a key algorithm that relates the first and second keys together;

(e) selecting from the plaintext file a block of binary data to be encrypted;

(f) selecting, according to the key algorithm, an integer value from the second key;

(g) inputting, according to the key algorithm, the integer value selected from the second key into the first key so as to obtain one or more integer values;

(h) performing an XOR process on the block of original binary data using the one or more integer values obtained from the first key so as to generate a block of encrypted binary data; and

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

(i) repeating steps (e)–(h) until a desired portion the plaintext file has been encrypted so as to yield a ciphertext file including blocks of encrypted binary data.

2. A method as defined in claim 1, wherein the blocks of original binary data to be encrypted are one byte in length and have a maximum numeric value of 255 and wherein the integer values included in the first key are selected from a set bounded below by 0 or 1 and bounded above by 255.

3. A method as defined in claim 1, wherein the integer values contained in the first key and the second key are random or pseudo-random numbers.

4. A method as defined in claim 1, wherein the number of integer values obtained from the first key and used in encrypting the block of original binary data is determined by a remainder value generated by dividing the integer value selected from the second key by a predetermined divisor.

5. A method as defined in claim 4, wherein the number of integer values within the first key is 2048, wherein the number of integer values within the second key is 2048, and wherein the predetermined divisor used to generate the remainder value is 20.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

6. A method as defined in claim 4, wherein the number of integer values obtained from the first key is equal to the remainder value except when the remainder value equals 0.

7. A method as defined in claim 1, wherein the first integer value selected from the second key when encrypting the first block of original binary data is selected from index position 0, wherein each successive integer value selected from the second key when encrypting each successive block of original binary data is selected by first updating each immediately preceding index position by the value of the immediately preceding block of encrypted binary data and then selecting the integer value contained in the updated index position, provided that when the updated index position exceeds the highest possible index position the index position is reset to 0 plus the number of times the highest possible index position has been exceeded, provided that when the number of times the highest possible index position has been exceeded exceeds the highest possible index position the index position is reset to 0.

8. A method as defined in claim 1, wherein the XOR process is modified so that it is not commutative.

9. A method as defined in claim 1, further including the step of storing the ciphertext file together with the first key so as to yield an encrypted file.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

10. A method as defined in claim 9, wherein the encrypted file is stored in a manner so as to have a unique suffix appended to the name of the encrypted file and thereby identify the encrypted file as being of a unique file type.

11. A method as defined in claim 10, further including the steps of sending to a decrypting party the encrypted file of the unique file type and providing the decrypting party with software capable of decrypting the encrypted file, so as to yield at least a portion of the plaintext file, and outputting data corresponding to information contained within the plaintext file.

12. A method as defined in claim 11, wherein the software limits or prevents copying, alteration or sending of the information contained within the plaintext file by the decrypting party.

13. A method as defined in claim 1, further including the steps of:

(j) providing to a decrypting party the ciphertext file including blocks of encrypted binary data to be decrypted, the first key, and the second key;

(k) selecting from the ciphertext file a block of encrypted binary data to be decrypted;

(l) selecting, according to the key algorithm, the integer value previously selected from the second key when encrypting the block of encrypted binary data in steps (e)–(h);

(m) inputting, according to the key algorithm, the integer value selected from the second key into the first key so as to obtain the one or more

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

integer values previously selected from the first key when encrypting the block of encrypted binary data in steps (e)-(h);

(n) performing an XOR process on the block of encrypted binary data using the one or more integer values obtained from the first key so as to restore the block of original binary data from which the block of encrypted binary data was generated; and

(o) repeating steps (k)–(n) until at least a portion of the ciphertext file has been decrypted so as to restore at least a portion of the plaintext file.

14. A method as defined in claim 13, wherein the ciphertext and first key are provided to the decrypting party by means of a transmission by an encrypting party over the Internet.

15. A method as defined in claim 15, wherein the ciphertext and first key are provided to the decrypting party by means of HTTPS.

16. A method as defined in claim 13, wherein the second key and key algorithm are provided to the decrypting party as part of a computer-readable medium.

17. A method as defined in claim 13, wherein the second key is provided to the decrypting party by means of a password protected login procedure over a secure line between the decrypting party and an encrypting party.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

18. A method as defined in claim 1, wherein the plaintext file is at least one of a graphic file or a text file.

19. A method as defined in claim 1, wherein the plaintext file digitally represents graphic information contained in a tangible document and is a TIFF file.

20. A method as defined in claim 1, wherein the plaintext file digitally represents graphic information contained in a tangible document and is at least one of a JPEG, BMP or GIF file.

21. A method as defined in claim 1, wherein at least one of the first and second keys is unique to the plaintext file.

22. A computerized system comprising means for implementing the method recited in at least one of claims 1 or 12.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

23. A computer-readable medium having computer-executable instructions for performing the steps of:

(a) providing a plaintext file that includes blocks of original binary data to be encrypted, said blocks having a given length and a maximum possible integer value;

(b) providing a first key that includes a number of indexed integer values selected from a set bounded below by 0 or 1 and above by the maximum possible integer value of the blocks of binary data to be encrypted;

(c) providing a second key that includes a number of indexed integer values selected from a set bounded below by 0 and above by the predetermined number of indexed integer values included in the first key;

(d) providing a key algorithm that relates the first and second keys together;

(e) selecting from the plaintext file a block of binary data to be encrypted;

(f) selecting, according to the key algorithm, an integer value from the second key;

(g) inputting, according to the key algorithm, the integer value selected from the second key into the first key so as to obtain one or more integer values;

(h) performing an XOR process on the block of original binary data using the one or more integer values obtained from the first key so as to generate a block of encrypted binary data; and

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

(i) repeating steps (e)–(h) until a desired portion the plaintext file has been encrypted so as to yield a ciphertext file including blocks of encrypted binary data.

24. A computer-readable medium, at least partially separate from the computer readable medium of claim 23, having computer-executable instructions for performing the steps of:

(j) providing to a decrypting party the ciphertext file, generated using the computer-readable medium of claim 23, including blocks of encrypted binary data to be decrypted, the first key, and the second key;

(k) selecting from the ciphertext file a block of encrypted binary data to be decrypted;

(l) selecting, according to the key algorithm, the integer value previously selected from the second key when encrypting the block of encrypted binary data in steps (e)–(h);

(m) inputting, according to the key algorithm, the integer value selected from the second key into the first key so as to obtain the one or more integer values previously selected from the first key when encrypting the block of encrypted binary data in steps (e)–(h);

(n) performing an XOR process on the block of encrypted binary data using the one or more integer values obtained from the first key so as to restore the block of original binary data from which the block of encrypted binary data was generated; and

(o) repeating steps (k)–(n) until at least a portion of the ciphertext file has been decrypted so as to restore at least a portion of the plaintext file.

25. A computer-readable medium as defined in claim 23, wherein at least one of the first and second keys is unique to the plaintext file.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

26. A method for protecting an electronic file sent over the Internet from unauthorized access, copying or alteration, comprising:

(a) encrypting a plaintext file using an encryption algorithm, a public key, and a private key so as to generate a ciphertext file;

(b) storing the ciphertext file together with the public key so as to yield a composite file of a unique file type;

(c) sending the composite file to an authorized decrypting party over the Internet;

(d) separately providing the decrypting party with the private key and a decryption algorithm corresponding to the encryption algorithm which, together with the public key provided as part of the composite file, allow the decrypting party to at least partially decrypt the ciphertext file and restore at least a portion of the plaintext file.

27. A method as defined in claim 26, wherein the private key and decryption algorithm are integrated together as part of a restricted output algorithm which inhibits or prevents copying, alteration and sending of the restored portion of the plaintext file.

28. A method as defined in claim 27, wherein the plaintext file digitally represents information contained in a tangible document and wherein the restricted output algorithm includes an algorithm for outputting at least a portion of the information contained in the tangible document.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

29. A method as defined in claim 28, wherein the plaintext file is at least one of a graphic file or a text file.

30. A method as defined in claim 28, wherein the plaintext file is a TIFF file.

31. A method as defined in claim 26, wherein at least one of the first and second keys is unique to the plaintext file.

32. A computerized system comprising means for implementing the method recited in claim 26.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

33. A method for decrypting an encrypted file while preventing or inhibiting copying, alteration or sending of decrypted plaintext data, comprising:

(a) providing a decrypting party with a ciphertext file, a decryption algorithm and key necessary to decrypt the ciphertext file so as to restore at least a portion of a plaintext file corresponding to the ciphertext file, and an output algorithm integrated with the decryption algorithm and key that permits at least one of viewing or printing of information relating to the plaintext file but which prevents or inhibits copying, alteration or transmission of said information;

(b) permitting the decrypting party to decrypt the ciphertext file using the decryption algorithm and key so as to restore at least a portion of the plaintext file corresponding to the ciphertext file, wherein the output algorithm permits at least one of viewing or printing of the information relating to the plaintext file but which prevents or inhibits copying, alteration or transmission of said information.

34. A method as defined in claim 33, wherein the decryption algorithm and output algorithm are provided to the decrypting party in the form of a computer-readable medium.

35. A method as defined in claim 33, wherein the ciphertext and a first portion of the key are provided to the decrypting party by means of a transmission from an encrypting party over the Internet and wherein a second portion of the key is separately provided to the decrypting party in a manner so that only the encrypting and decrypting parties have access to the private key.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

36. A method as defined in claim 35, wherein the second portion of the key is provided to the decrypting party together with the decryption algorithm.

37. A method as defined in claim 35, wherein the second portion of the key is provided to the decrypting party by means of a password-protected login procedure.

38. A method as defined in claim 35, wherein at least one of the first and second portions of the key is unique to the plaintext file.

39. A computerized system comprising means for implementing the method recited in claim 33.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111